
Article:
Lupo, Cosmo orcid.org/0000-0002-5227-4009, Ottaviani, Carlo orcid.org/0000-0002-0032-3999, Papanastasiou, Panagiotis et al. (1 more author) (2018) Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. Physical Review A. 052327. pp. 1-10. ISSN 1094-1622

https://doi.org/10.1103/PhysRevA.97.052327

Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks

Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, United Kingdom

(Received 22 December 2017; revised manuscript received 24 April 2018; published 29 May 2018)

We present a rigorous security analysis of continuous-variable measurement-device-independent quantum key distribution (CV MDI QKD) in a finite-size scenario. The security proof is obtained in two steps: by first assessing the security against collective Gaussian attacks, and then extending to the most general class of coherent attacks via the Gaussian de Finetti reduction. Our result combines recent state-of-the-art security proofs for CV QKD with findings about min-entropy calculus and parameter estimation. In doing so, we improve the finite-size estimate of the secret key rate. Our conclusions confirm that CV MDI protocols allow for high rates on the metropolitan scale, and may achieve a nonzero secret key rate against the most general class of coherent attacks after 10^7–10^9 quantum signal transmissions, depending on loss and noise, and on the required level of security.

DOI: 10.1103/PhysRevA.97.052327

I. INTRODUCTION

Quantum communication technologies, and in particular quantum key distribution (QKD), are rapidly progressing from research laboratories towards real-world implementations. The ultimate goal is building a network of quantum devices (quantum internet) enabling unconditionally secure communications on the global scale [1–4]. To this end, QKD has been recently extended to a scenario where two honest users (Alice and Bob) exploit the mediation of an untrusted relay, operated by the eavesdropper (Eve), to establish a secure communication channel [5,6]. This remarkable feature is made possible by the working mechanism of the relay itself, which activates secret correlations on the users' remote stations by performing Bell detection on the incoming signals and publicly announcing the results [6]. This architecture has been called measurement-device-independent (MDI) QKD because, as such, the security of the communication does not rely on the assumption that the measurement devices (which are more exposed to side-channel attacks than other devices) are trusted [5,6].

Protocols exploiting quantum continuous variables have attracted considerable attention for their potential of boosting the communication rate and for their employability across midrange (metropolitan) distances [6,7]. The key rates achievable by continuous-variable (CV) QKD protocols are not far from the ultimate repeaterless bound for private communication, which, for a lossy line of transmissivity η is $-\log(1-\eta)$ bits per use [8]. The security of CV QKD, which is very well established under Gaussian attacks and in the asymptotic regime [9], has been recently generalized to the most general class of coherent attacks as well as to the finite-size setting [10–14]. In this landscape, the problem of establishing the secret key rates achievable by CV MDI QKD in the finite-size setting has not been yet explicitly addressed.

In this paper we fill this gap and provide a rigorous composable-security proof of the CV MDI QKD protocol proposed in Ref. [6] (this proof can then be extended to tripartite [15] and multipartite CV MDI protocols [16]). The security of CV MDI QKD against collective attacks can be obtained along the lines of Ref. [10]. Then, the extension to the most general class of coherent attacks can be obtained by exploiting the recently introduced Gaussian de Finetti reduction [11]. Here we apply to CV MDI QKD and improve the proof techniques of Ref. [10]:

(1) We present a simpler analysis of parameter estimation that holds under general coherent attacks. Our analysis exploits the recently proven optimality of Gaussian attacks in the finite-size scenario [11] to simplify parameter estimation.

(2) We show that in CV MDI protocols the parameter estimation routine can be performed locally by the legitimate users with almost no public communication.

(3) We improve the secret-key rate estimates of Ref. [10] by exploiting a different entropic inequality.

The paper develops as follows. We start in Sec. II by reviewing the CV MDI QKD protocol of Ref. [6]. Section III is devoted to our results about parameter estimation and its statistical analysis. In Sec. IV we present an improved estimation of the secret-key rate obtained by applying a new entropic inequality. A comparison with previous works is presented in Sec. V. To make our results more concrete, numerical examples are presented in Sec. VI. We finally discuss the relation between security proof and experimental realization and possible improvements in Sec. VII. Finally, conclusions are presented in Sec. VIII.

II. DESCRIPTION OF THE PROTOCOL

In this section, we review the CV MDI QKD protocol introduced in Ref. [6]. The protocol develops in five steps (see Fig. 1):

(1) *Coherent states preparation.* Alice and Bob locally prepare $2n$ coherent states, whose complex amplitudes $\alpha' = (q'_A + ip'_A)/2$ and $\beta' = (q'_B + ip'_B)/2$ are drawn independent and identically distributed (i.i.d.) from circular symmetric, zero-mean Gaussian distributions with variance V_M^A and V_M^B,

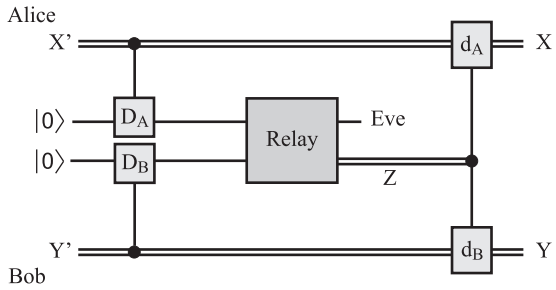

FIG. 1. The scheme of the CV MDI QKD protocol as described in detail in Sec. II. Single lines represent bosonic modes, double lines classical variables. Time evolves from left to right. Alice and Bob initially prepare coherent states by applying displacement operators D_A, D_B to the vacuum state $|0\rangle$, according to the value of their local classical variables. The coherent states are collected by the relay that, through some (unknown) physical transformation, outputs a classical variable Z and gives to Eve quantum side information. Finally, Alice and Bob apply *classical* displacement d_A, d_B, conditioned on the value of Z, to their local classical variables.

respectively [17]. The initial random variables of Alice and Bob are respectively denoted as $X' = (q'_A, p'_A)$, $Y' = (q'_B, p'_B)$.

(2) *Operations of the relay.* The $2n$ coherent states are sent to the relay. For each pair of coherent states received the relay publicly announces a complex value $\gamma = (q_Z + ip_Z)/2$.

(3) *Parameter estimation.* Alice and Bob estimate the covariance matrix (CM) of the variables $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$.

(4) *Conditional displacements.* Alice and Bob define the displaced variables $\alpha = (q_A + ip_A)/2$ and $\beta = (q_B + ip_B)/2$ such that

$$q_A = q'_A - g_{q'_A}(\gamma), \tag{1}$$

$$p_A = p'_A - g_{p'_A}(\gamma), \tag{2}$$

$$q_B = q'_B - g_{q'_B}(\gamma), \tag{3}$$

$$p_B = p'_B - g_{p'_B}(\gamma), \tag{4}$$

where $g_\star$, for each $\star = q'_A, p'_A, q'_B, p'_B$, is an affine function of γ. As shown in Ref. [19], the optimal choice is to define the functions as

$$g_\star(\gamma) = u_\star q_Z + v_\star p_Z, \tag{5}$$

where [20]

$$u_\star = \frac{\langle \star\, q_Z\rangle\langle p_Z^2\rangle - \langle \star\, p_Z\rangle\langle q_Z p_Z\rangle}{\langle p_Z^2\rangle\langle q_Z^2\rangle - \langle q_Z p_Z\rangle^2}, \tag{6}$$

$$v_\star = \frac{\langle \star\, p_Z\rangle\langle q_Z^2\rangle - \langle \star\, q_Z\rangle\langle q_Z p_Z\rangle}{\langle q_Z^2\rangle\langle p_Z^2\rangle - \langle q_Z p_Z\rangle^2}. \tag{7}$$

We remark that the parameters $u_\star$, $v_\star$ can be computed directly from the estimated CM.

(5) *Classical postprocessing.* The variables $X = (q_A, p_A)$, $Y = (q_B, p_B)$ represent the local raw keys of Alice and Bob, respectively. To conclude the protocol, the raw keys X, Y are postprocessed for error correction and privacy amplification. We assume without loss of generality that error reconciliation is on Alice's raw key.

The CV MDI QKD protocol described above has two main characteristic features. The first is that Alice and Bob do not apply any measurement, as the only measurement is performed by the untrusted relay. This property defines the protocol as MDI [5,6]. The second feature is that the correlations between Alice and Bob are generated through the variable Z announced by the relay. As explained in detail in Ref. [19], this property allows Alice and Bob to do parameter estimation with a negligible amount of public communication [21]. Therefore, they can exploit the whole raw key for both parameter estimation and secret-key extraction.

Finally we remark that, although the variables X and Y have in principle infinite cardinality, in practice they are always specified by a finite number of digits. Furthermore, for the finite-size analysis of the protocol (as well as for other practical issues), one needs to map the unbounded and continuous variables X, Y to some discrete and bounded variables $\bar{X}$, $\bar{Y}$. The mappings $X \to \bar{X}$, $Y \to \bar{Y}$ can be realized by an analog-to-digital conversion (ADC) algorithm. We therefore assume that $\bar{X}$ and $\bar{Y}$ are discrete variables with cardinality 2^{2d} (i.e., d bits per quadrature).

III. PARAMETER ESTIMATION

In this section we discuss how Alice and Bob can estimate the CM of the variables (q_A, p_A, q_B, p_B). Without loss of generality we can assume that these variables have zero mean and the CM has the form

$$\mathbf{V}_{AB} = \left\langle \begin{pmatrix} q_A^2 & q_A p_A & q_A q_B & q_A p_B \\ p_A q_A & p_A^2 & p_A q_B & p_A p_B \\ q_B q_A & q_B p_A & q_B^2 & q_B p_B \\ p_B q_A & p_B q_B & p_B q_B & p_B^2 \end{pmatrix} \right\rangle = \begin{pmatrix} x\mathbf{I} & z\mathbf{I} \\ z\mathbf{I} & y\mathbf{I} \end{pmatrix}, \tag{8}$$

where $\mathbf{I} = \mathrm{diag}(1,1)$, and

$$x = \frac{\langle q_A^2\rangle + \langle p_A^2\rangle}{2}, \tag{9}$$

$$y = \frac{\langle q_B^2\rangle + \langle p_B^2\rangle}{2}, \tag{10}$$

$$z = \frac{\langle q_A q_B\rangle + \langle p_A p_B\rangle}{2}. \tag{11}$$

Clearly, the entries on the principal diagonal of (8) can be estimated locally by either Alice or Bob. It remains to estimate the off-diagonal term z. This can be done in three different ways:

(1) The traditional way is that Alice and Bob exchange part of the data via a public channel to estimate the correlation terms $\langle q_A q_B\rangle$ and $\langle p_A p_B\rangle$. Clearly, in order to do so they have to disclose part of the raw key, thus reducing the final secret-key rate. Suppose that, over a total of n signals exchanged, Alice and Bob use $m < n$ signals for parameter estimation, thus allowing an error in the estimation of the order of $m^{-1/2}$. Then only the remaining $n - m < n$ signals are available for secret-key extraction (i.e., error correction and privacy amplification).

(2) As noted in Ref. [10] (see also Ref. [22]) a rough estimate of the signal-to-noise ratio is sufficient for Alice and Bob to run the error correction routine before performing

parameter estimation. Then, a verification step is done to ensure that the initial estimate was accurate enough. In this way Alice and Bob can exploit virtually all the raw data for key generation.

(3) For our MDI protocol Alice and Bob can exploit the relations (see Sec. II)

$$q_A = q'_A - u_{q'_A} q_Z - v_{q'_A} p_Z, \tag{12}$$

$$p_A = p'_A - u_{p'_A} q_Z - v_{p'_A} p_Z, \tag{13}$$

$$q_B = q'_B - u_{q'_B} q_Z - v_{q'_B} p_Z, \tag{14}$$

$$p_B = p'_B - u_{p'_B} q_Z - v_{p'_B} p_Z, \tag{15}$$

to obtain

$$\begin{aligned} z &= \frac{\langle q_A q_B \rangle + \langle p_A p_B \rangle}{2} \\ &= w_1 \langle q_Z^2 \rangle + w_2 \langle p_Z^2 \rangle + w_3 \langle q_Z p_Z \rangle, \end{aligned} \tag{16}$$

where we have defined

$$w_1 := \tfrac{1}{2}\left(u_{q'_A} u_{q'_B} + u_{p'_A} u_{p'_B}\right), \tag{17}$$

$$w_2 := \tfrac{1}{2}\left(v_{q'_A} v_{q'_B} + v_{p'_A} v_{p'_B}\right), \tag{18}$$

$$w_3 := \tfrac{1}{2}\left(u_{q'_A} v_{q'_B} + v_{q'_A} u_{q'_B} + u_{p'_A} v_{p'_B} + v_{p'_A} u_{p'_B}\right). \tag{19}$$

Since the variances $\langle q_Z \rangle$, $\langle p_Z \rangle$ and the covariance $\langle q_Z p_Z \rangle$ can be locally computed by the users, then this implies that Alice and Bob can do parameter estimation without publicly announcing their local data [21]. In conclusion, in this way Alice and Bob can exploit all their raw data for both parameter estimation and secret-key extraction.

Here we follow the latter approach because, in contrast with the first approach and in analogy with the second one, it requires only a constant (and hence negligible) amount of public communication. Furthermore, the third approach exploits the very structure of the MDI protocol and therefore appears to be the most natural in this context.

Statistical analysis of parameter estimation

We are then left with the problem of estimating the confidence interval associated with the statistical estimation of the CM of (q_A, p_A, q_B, p_B). It is worth stressing that this is a remarkably complex problem in the case of general collective attacks (see Ref. [10]). By contrast, this task becomes straightforward under the assumption of collective Gaussian attacks. Unlike other authors [23–25], our analysis of parameter estimation under collective Gaussian attacks does not rely on the central limit theorem and is therefore mathematically rigorous in the finite-size setting (see instead Refs. [26,27] for a statistical analysis of parameter estimation in CV MDI QKD that exploits the central limit theorem).

Our analysis is based on the assumption that the $(q'_A, p'_A, q'_B, p'_B, q_Z, p_Z)$ are Gaussian variables. This assumption comes with no loss of generality because

(i) The variables (q'_A, p'_A, q'_B, p'_B) are Gaussian by definition of the protocol.

(ii) The optimality of Gaussian attacks in the finite-size scenario was established in Ref. [11]. This implies that the variables (q_A, p_A, q_B, p_B) can be assumed to be Gaussian without loss of generality.

(iii) In principle, the variables (q_Z, p_Z) are not necessarily Gaussian. Notwithstanding, by inverting Eqs. (12)–(15) we can write (q_Z, p_Z) as linear combinations of (q_A, p_A, q_B, p_B) and (q'_A, p'_A, q'_B, p'_B). Since the latter are assumed to be Gaussian, and since a linear combination of Gaussian variables is also Gaussian, it follows that (q_Z, p_Z) are Gaussian variables too.

First consider the estimation of, say, $\langle q_Z^2 \rangle$, whose estimator is the empirical variance $n^{-1} \sum_{j=1}^n q_{Zj}^2$. Given that q_{Zj} are i.i.d. Gaussian variables [28], then the empirical variance is distributed (up to rescaling) according to a χ-squared distribution. Therefore, a confidence interval can be readily obtained applying the cumulative distribution function of the χ-squared distribution, or tail bounds for it.

Second, consider the estimation of the correlation $\langle q_Z p_Z \rangle$. We apply the identity

$$\langle q_Z p_Z \rangle = \tfrac{1}{4} \langle (q_Z + p_Z)^2 \rangle - \tfrac{1}{4} \langle (q_Z - p_Z)^2 \rangle, \tag{20}$$

whose estimator

$$\frac{1}{n} \sum_{j=1}^n q_{Zj} p_{Zj} = \frac{1}{4n} \sum_{j=1}^n (q_{Zj} + p_{Zj})^2 - \frac{1}{4n} \sum_{j=1}^n (q_{Zj} - p_{Zj})^2 \tag{21}$$

is distributed as the sum of χ-squared variables. Therefore, for each χ-squared variable, we can compute a confidence interval and then obtain a confidence interval for the quantities x, y, and z in Eq. (8) by error propagation.

An explicit calculation of the confidence intervals is presented in Appendix C.

IV. IMPROVED RATE ESTIMATION

The security proof against collective or Gaussian attacks can be obtained along the lines of Ref. [10]. Here we present an improved estimation of the conditional smooth min-entropy obtained by applying a new entropic inequality.

We assume without loss of generality that the reconciliation is on Bob's variable $\bar{Y}$. The number of (approximately) secret bits that can be extracted from the raw key is lower bounded by the smooth min-entropy of $\bar{Y}$, conditioned on the quantum state of the eavesdropper E' as well as on the classical variable Z [29]:

$$s_n^{\epsilon+\epsilon_s+\epsilon_{\rm EC}} \geqslant H_{\min}^{\epsilon_s}(\bar{Y}|E'Z)_{\rho^n} - {\rm leak}_{\rm EC}(n, \epsilon_{\rm EC}) + 2\log(2\epsilon), \tag{22}$$

where we have also subtracted the information leakage ${\rm leak}_{\rm EC}(n, \epsilon_{\rm EC})$ due to error correction (EC). The security parameter $\epsilon + \epsilon_s + \epsilon_{\rm EC}$ comprises three terms: ϵ comes from the leftover hash lemma, ϵ_s is the smoothing parameter entering the smooth conditional min-entropy, and $\epsilon_{\rm EC}$ is the error in the error-correction routine. Since conditioning does not increase the entropy, for any purification ρ_{ABE}^n of $\rho_{ABE'Z}^n$ we have

$$H_{\min}^{\epsilon_s}(\bar{Y}|E'Z)_{\rho^n} \geqslant H_{\min}^{\epsilon_s}(\bar{Y}|E)_{\rho^n}, \tag{23}$$

which implies

$$s_n^{\epsilon+\epsilon_s+\epsilon_{\rm EC}} \geqslant H_{\min}^{\epsilon_s}(\bar{Y}|E)_{\rho^n} - {\rm leak}_{\rm EC}(n,\epsilon_{\rm EC}) + 2\log(2\epsilon). \tag{24}$$

A crucial point of the security proof is the estimation of the conditional smooth min-entropy $H_{\min}^{\epsilon_s}(\bar{Y}|E)_{\rho^n}$. Here we present an approach that yields a bound on the min-entropy that is tighter than the one of Ref. [10]. For collective (or collective Gaussian) attacks, the state ρ^n is a tensor power; i.e., $\rho^n = \rho^{\otimes n}$. On the other hand, the state that is actually used for key generation is the one conditioned upon error correction being successful. Because error correction has a nonzero failure probability, the conditional state is no longer guaranteed to be a tensor power. Indeed, the conditioned state has the form

$$\tau^n = p^{-1}\Pi\rho^{\otimes n}\Pi, \tag{25}$$

where Π is a projector operator (projecting on the subspace in which error correction does not abort), and $p = {\rm Tr}(\Pi\rho^{\otimes n}\Pi)$ is the probability of successful error correction. Let us recall that the security parameter ϵ can be interpreted as the probability that the protocol is not secure (see Appendix A for a review). Therefore, the probability that the protocol is not secure, given that it does not abort, cannot be larger than ϵ/p. This suggests a relation of the form

$$H_{\min}^{\epsilon}(\bar{Y}|E)_{\tau^n} \simeq H_{\min}^{p\epsilon}(\bar{Y}|E)_{\rho^{\otimes n}}. \tag{26}$$

The following theorem holds:

Theorem 1. Given two n-qudit states τ^n and $\rho^{\otimes n}$ such that $\tau^n = p^{-1}\Pi\rho^{\otimes n}\Pi$ for some projector operator Π and $p = {\rm Tr}(\Pi\rho^{\otimes n})$, then

$$H_{\min}^{\epsilon}(\bar{Y}|E)_{\tau^n} \geqslant H_{\min}^{\frac{2}{3}p\epsilon}(\bar{X}|E)_{\rho^{\otimes n}} + \log\left(p - \frac{2}{3}p\epsilon\right). \tag{27}$$

The proof is presented in Appendix B.

Theorem 1 implies that the state can still be assumed to be a tensor power upon replacing $\epsilon \to \frac{2}{3}p\epsilon$ and shortening the secret key by $\log\left(p - \frac{2}{3}p\epsilon\right)$ bits, that is,

$$\begin{aligned} s_n^{\epsilon+\epsilon_s+\epsilon_{\rm EC}} \geqslant & H_{\min}^{\frac{2}{3}p\epsilon_s}(\bar{Y}|E)_{\rho^{\otimes n}} - {\rm leak}_{\rm EC}(n,\epsilon_{\rm EC}) \\ & + \log\left(p - \frac{2}{3}p\epsilon_s\right) + 2\log(2\epsilon). \end{aligned} \tag{28}$$

The conditional smooth min-entropy of the tensor-power state $\rho^{\otimes n}$ can be estimated using the asymptotic equipartition property (AEP), which yields a bound in terms of the von Neumann conditional entropy [30]:

$$H_{\min}^{\delta}(\bar{Y}|E)_{\rho^{\otimes n}} \geqslant nH(\bar{Y}|E)_{\rho} - \sqrt{n}\,\Delta_{\rm AEP}(\delta,d),$$

where

$$\Delta_{\rm AEP}(\delta,d) \leqslant 4(d+1)\sqrt{\log(2/\delta^2)} \tag{29}$$

is also a function of the dimensionality parameter d.

The next step in the security proof is to estimate the conditional entropy

$$H(\bar{Y}|E)_{\rho} = H(\bar{Y})_{\rho} - I(\bar{Y};E)_{\rho}. \tag{30}$$

Let us first consider the estimation of the mutual information $I(\bar{Y};E)_{\rho}$. We remark that the latter is upper bounded by the mutual information with the variable Y, i.e., $I(\bar{Y};E)_{\rho} \leqslant I(Y;E)_{\rho}$, since the ADC algorithm cannot increase the mutual information. In turn, the property of extremality of Gaussian states [31,32] allows us to write the bound $I(Y;E)_{\rho} \leqslant I(Y;E)_{\rho_G} \equiv I_{BE}$, where ρ_G is a Gaussian state with same CM as ρ.

To conclude, we notice that the quantity $nH(\bar{Y}) - {\rm leak}_{\rm EC}(n,\epsilon_{\rm EC})$ is the number of (not necessarily secret) bits of common information shared by Alice and Bob after the error-correction routine. Ideally, in the limit of large block size, ADC with arbitrarily large precision, and perfect operations, this quantity is expected to be equal to $nI(X;Y)_{\rho}$, where $I(X;Y)$ is the mutual information between Alice and Bob. Therefore, we can put

$$H(\bar{Y}) - \frac{1}{n}{\rm leak}_{\rm EC}(n,\epsilon_{\rm EC}) = \beta I(X;Y)_{\rho}, \tag{31}$$

where the efficiency parameter $\beta \in (0,1)$ accounts for all the sources of nonideality in the protocol. The inequality $\beta I(X;Y)_{\rho} \geqslant \beta I(X;Y)_{\rho_G} \equiv \beta I_{AB}$, where ρ_G is the Gaussian state with same first and second moments, follows from Ref. [32]. Notice that β is also a function of n and $\epsilon_{\rm EC}$.

In conclusion, the results presented in this section, combined with the security proof of Ref. [10], yield the following lower bound on the secret-key rate:

$$r_n^{\epsilon+\epsilon_s+\epsilon_{\rm EC}+\epsilon_{\rm PE}} = \frac{1}{n}\, s_n^{\epsilon+\epsilon_s+\epsilon_{\rm EC}+\epsilon_{\rm PE}} \tag{32}$$

$$\begin{aligned} \geqslant & \beta\hat{I}_{AB} - \hat{I}_{BE} - \frac{1}{\sqrt{n}}\,\Delta_{\rm AEP}\left(\frac{2}{3}p\epsilon_s, d\right) \\ & + \frac{1}{n}\log\left(p - \frac{2}{3}p\epsilon_s\right) + \frac{1}{n}\,2\log(2\epsilon), \end{aligned} \tag{33}$$

where $\hat{I}_{AB}$ and $\hat{I}_{BE}$ are the empirical estimates for the mutual informations, and $\epsilon_{\rm PE}$ is the probability of error in parameter estimation.

V. COMPARISON WITH PREVIOUS SECURITY PROOF

Our expression for the rate in Eq. (33) can be compared to the analogous expression given in Theorem 1 of Ref. [10]. The first difference between the two expressions is in the term proportional to $\Delta_{\rm AEP}$ (that is the leading correction term in our finite-size analysis), which in Ref. [10] is replaced by [33]

$$\Delta_{\rm AEP}^{(1)} = (d+1)^2 + 4(d+1)\sqrt{\log\frac{2}{\epsilon^2}} + 2\log\frac{2}{p^2\epsilon} + 4\frac{\epsilon d}{p\sqrt{n}}. \tag{34}$$

It is clear that $\Delta_{\rm AEP}^{(1)} > \Delta_{\rm AEP}$, where for small values of p and ϵ the difference is dominated by the term $2\log\frac{2}{p^2\epsilon}$. We emphasize that the fact that with our approach we obtain a smaller finite-size correction $\Delta_{\rm AEP}$ follows from the application of the min-entropy inequality of Theorem 1.

The expression for the rate in Ref. [10] also includes an additional error term $\Delta_{\rm ent}$, scaling as $n^{-1/2}\log n$. In our formulation this term does not appear and has been somehow incorporated in the efficiency factor β. We believe that our approach provides a better way to model what is done in experimental implementations of the protocol. We remark that

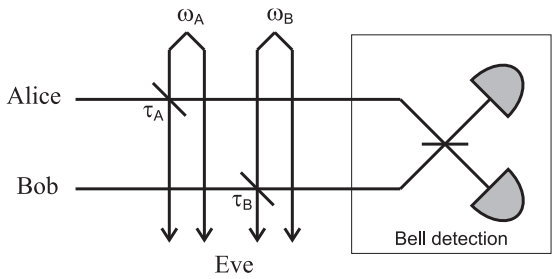

FIG. 2. As an example, in Sec. VI we consider the case of independent entangling cloner attacks on the two communication lines, where τ_A and τ_B are the beam-splitter transmissivities. The attacks also introduce independent excess noises of variances $\xi_A = (1-\tau_A)(\omega_A - 1)$, $\xi_B = (1-\tau_B)(\omega_B - 1)$. The relay applies Bell detection on the incoming modes, whose result defines the variable Z and is publicly announced.

Δ_{ent} is the leading finite-size correction term in the analysis of Ref. [10].

Finally, we exploit the Gaussian assumption to compute the confidence intervals for parameter estimation. The result (see Appendix C) is that the elements of the CM can be estimated up to a relative error of the order of

$$\sqrt{\frac{8\ln(8/\epsilon_{\text{PR}})}{n}} \tag{35}$$

with a given overall probability of error smaller than ϵ_{PR}. This result is comparable with that of Ref. [10]: the reason is that, although Ref. [10] considers general collective attacks, the analysis of the parameter estimation is effectively reduced to the Gaussian setting by applying a randomization technique. Although we obtain finite-size corrections related to parameter estimation that are quantitatively similar to Ref. [10], our statistical analysis is much simpler. This is due to the fact that we exploit the assumption of a Gaussian attack which has been proven to come without loss of generality even in the finite-size setting [11].

VI. NUMERICAL EXAMPLES

The expression in Eq. (33), together with the parameter estimation analysis of Sec. III, allows us to compute the estimated secret key directly from experimental data for any Gaussian attack (and then extend to general attacks using the results of Ref. [11]). In this section, as an example, we compute the rate as a function of loss and block size for the case of an entangling cloner attack (depicted in Fig. 2). We consider two settings: (1) symmetric attacks in which both communication lines from Alice to the relay and from Bob to the relay are wiretapped with a beam splitter with equal transmissivity $\tau_A = \tau_B = \tau$, and (2) asymmetric attacks where the relay is assumed very close to Alice's station, $\tau_A \simeq 1$.

In both cases, following Ref. [6], the eavesdropper collects all the loss from the communication lines, and the variable Z is the outcome of a perfect Bell detection performed at the relay. These kinds of attacks have been characterized thoroughly in Ref. [6], where the asymptotic rate (in the limit of infinite block size) has been computed as

$$r_n^0 = \beta \hat{I}_{AB} - \hat{I}_{BE}, \tag{36}$$

where the mutual informations are bounded by the results of parameter estimation. In our example we choose the conservative value $\beta = 0.95$ [34–37]. (Notice that in principle the factor β is a function of n and ϵ_{EC}, but for the sake of illustration we assume it to be constant.)

Putting $\langle q_A'^2\rangle = \langle p_A'^2\rangle = \langle q_B'^2\rangle = \langle p_B'^2\rangle = V_M$, we obtain

$$\langle q_A' q_Z\rangle = -\sqrt{\frac{\tau_A}{2}}\, V_M, \tag{37}$$

$$\langle p_A' p_Z\rangle = \sqrt{\frac{\tau_A}{2}}\, V_M, \tag{38}$$

$$\langle q_B' q_Z\rangle = \langle p_B' q_Z\rangle = \sqrt{\frac{\tau_B}{2}}\, V_M, \tag{39}$$

and the covariances of mutually conjugate quadratures vanish. We also have $\langle q_Z p_Z\rangle = 0$ and

$$\langle q_Z^2\rangle = \langle p_Z^2\rangle = \frac{\tau_A+\tau_B}{2} V_M + 1 + \frac{\xi_A+\xi_B}{2} =: \nu, \tag{40}$$

where $\xi_A = (1-\tau_A)(\omega_A - 1)$, $\xi_B = (1-\tau_B)(\omega_B - 1)$ are the excess noise variances and $\omega_{A,B}$ are the thermal noise that Eve injects in the links, respectively (see Eq. (1) of Ref. [6]). The only nonvanishing displacement coefficients are

$$u_{q_A'} = -\sqrt{\frac{\tau_A}{2}}\,\frac{V_M}{\nu}, \tag{41}$$

$$v_{p_A'} = \sqrt{\frac{\tau_A}{2}}\,\frac{V_M}{\nu}, \tag{42}$$

$$u_{q_B'} = v_{p_B'} = \sqrt{\frac{\tau_B}{2}}\,\frac{V_M}{\nu}, \tag{43}$$

that imply

$$w_1 = w_2 = -\frac{\sqrt{\tau_A\tau_B}}{4}\,\frac{V_M^2}{\nu^2}, \tag{44}$$

and $w_3 = 0$. Finally, applying Eq. (C9) we obtain

$$z_{\min} = \frac{\sqrt{\tau_A\tau_B}}{2(1+t)}\,\frac{V_M^2}{\nu}, \tag{45}$$

and similarly, from Eq. (C8),

$$x_{\max} = \frac{V_M}{1-t}\left(1 - \frac{\tau_A}{2}\frac{V_M}{\nu}\right), \tag{46}$$

$$y_{\max} = \frac{V_M}{1-t}\left(1 - \frac{\tau_B}{2}\frac{V_M}{\nu}\right), \tag{47}$$

with $t = \sqrt{n^{-1}\,8\ln(8/\epsilon_{\text{PE}})}$ (see Appendix C).

For collective Gaussian attacks, Eq. (33) is rewritten as

$$r_n^{\epsilon'} \geqslant r_n^0 - \frac{1}{\sqrt{n}}\,\Delta_{\text{AEP}}\left(\frac{2}{3}p\epsilon_s, d\right) + \frac{1}{n}\log\left(p - \frac{2}{3}p\epsilon_s\right) + \frac{1}{n}\,2\log(2\epsilon), \tag{48}$$

where $\epsilon' = \epsilon + \epsilon_s + \epsilon_{\text{EC}} + \epsilon_{\text{PE}}$. In Figs. 3 and 4 this rate is plotted vs the block size n, for different values of the transmissivities and excess noise for error-correction efficiency of $\beta = 95\%$. The plots are obtained putting $p = 0.99$, $\epsilon = \epsilon_s = \epsilon_{\text{EC}} = \epsilon_{\text{PE}} = 10^{-21}$, hence obtaining an overall security parameter $\epsilon' < 10^{-20}$. We also put $d = 5$: with this choice of

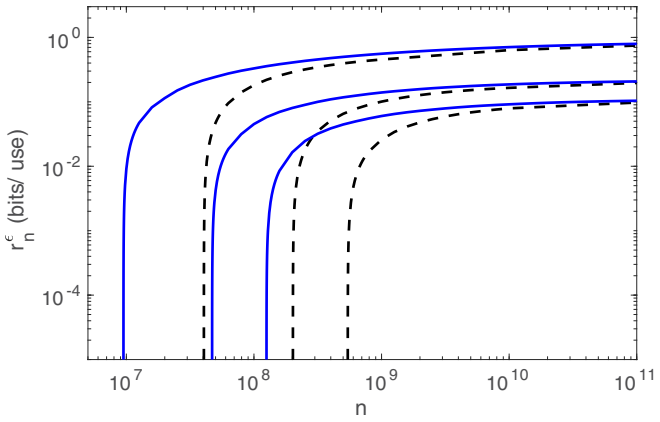

FIG. 3. Secret-key rate vs block size for asymmetric attacks: $\tau_A = 0.99$ and different values of τ_B (from top to bottom the attenuation of the communication line from Bob to the relay is of 1, 2, and 4 dB). The excess noise is $\xi_A = 0$ and $\xi_B = 0.01$ (in shot noise units). Solid lines are for collective Gaussian attacks, and dashed lines are for coherent attacks. For both kinds of attack, the overall security parameter is smaller than 10^{-20}.

d the error in the Shannon entropy due to the ADC is less than 1%. The rate is then obtained by maximizing over the value of modulation, V_M.

For coherent attacks, by applying the results of Ref. [11] we obtain

$$r_n^{\epsilon''} \geqslant \frac{n-k}{n} r_n^0 - \frac{\sqrt{n-k}}{n} \Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon_s, d\right) + \frac{1}{n}\log\left(p - \frac{2}{3}p\epsilon_s\right) + \frac{1}{n}2\log(2\epsilon) - \frac{1}{n}2\log\binom{K+4}{4}, \tag{49}$$

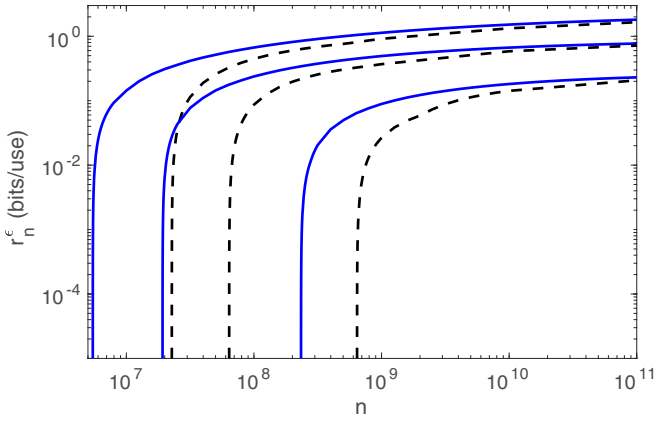

FIG. 4. Secret-key rate vs block size for symmetric attacks and different values of $\tau_A = \tau_B$ (from top to bottom the symmetric attenuation is of 0.1, 0.3, 0.5, and 0.55 dB). The excess noise is $\xi_A = \xi_B = 0.01$ (in shot noise units). Solid lines are for collective Gaussian attacks, and dashed lines are for coherent attacks. For both kinds of attack, the overall security parameter is smaller than 10^{-20}.

where k is the number of signals used for the energy test, $K \sim n$, and $\epsilon'' = \frac{K^4}{50}\epsilon'$.

In Figs. 3 and 4 this rate is plotted vs the block size n for different values of the transmissivities and excess noise, for error-correction efficiency of $\beta = 95\%$. The plots are obtained for $\epsilon = \epsilon_s = \epsilon_{\mathrm{EC}} = \epsilon_{\mathrm{PE}}$ chosen in such a way to obtain $\epsilon'' < 10^{-20}$. The rate is then obtained by maximizing over k and the modulation V_M and for $p = 0.99$.

VII. DISCUSSION

In the case of coherent attacks, the major bottleneck limiting the rate of secret bits generation *per second* comes from the classical postprocessing, and in particular the active symmetrization routine, due to the typically large size of the data set. While it has been conjectured that such an active symmetrization might not be actually needed [11], it remains an open theoretical problem to find a security proof that does not require one to perform such a computationally costly operation.

Here we present two arguments supporting the conjecture that the active symmetrization routine may not be actually performed in any experimental realization of the protocol:

(1) The active symmetrization routine consists in Alice and Bob multiplying their local raw keys by a random matrix. Since the matrix is invertible and publicly known, such an operation cannot by any means increase the secret-key length. Therefore, we deduce that the same secret-key rate might be achieved even without performing the symmetrization routine.

(2) The symmetrization routine is also instrumental for the energy test. After the symmetrization operation, Alice and Bob estimate the expectation value of the energy from only a relatively small part of the raw key. We notice that Alice and Bob can obtain an even better estimate of the mean energy from the whole raw key. This suggests that the symmetrization step might be avoided without affecting the energy test.

In summary, these two arguments suggest that the requirement of performing the symmetrization routine might be an artifact of the particular technique used to prove the security and therefore might not be strictly required in a practical realization of the protocol.

VIII. CONCLUSIONS

We have presented a rigorous assessment of the security of continuous-variable measurement-device-independent quantum key distribution (CV MDI QKD) in the finite-size regime. Our results are obtained by applying and modifying the results of Ref. [10], also exploiting the Gaussian de Finetti reduction recently introduced in Ref. [11], together with our results on parameter estimation and a new min-entropy inequality. Because of this improvement, our estimate on the secret-key rate is improved with respect to results of Refs. [10,11].

In doing this, we have shown that for our MDI protocol all the raw data can be used for both parameter estimation and secret-key extraction. Such a unique feature is a consequence of the fact that correlations between Alice and Bob are encoded in the variable that is publicly announced by the relay—even though such a variable does not contain information about the secret key (see Ref. [19]). It might be possible that for

the same reason the security analysis of MDI QKD can be further simplified, in particular the energy test and active symmetrization routines. It is worth remarking that standard one-way protocols, in both direct and reverse reconciliation, can be simulated by an MDI one, simply by assigning the relay to either Alice or Bob [6]. For this reason, this unique property of MDI QKD can be readily extended to the one-way setting [19].

Our statistical analysis of parameter estimation is fully composable and does not rely on the central limit theorem (and therefore is mathematically rigorous in the finite-size setting). Notwithstanding, we do not expect that our approach gives tight bounds on the statistical error induced by parameter estimation. In fact, tighter bounds may be obtained following a different approach, for example, by invoking the central limit theorem as in Refs. [26,27].

We have shown that it is in principle possible to generate a secret key against the most general class of coherent attacks for block sizes of the order of 10^7–10^9, depending on loss and noise, and on the required level of security. Therefore, our results indicate that a field demonstration of CV MDI QKD might be feasible with currently available technologies. In particular, our composable security analysis confirms that CV MDI protocols allow for high QKD rates on the metropolitan scale, thus confirming the results of the asymptotic analysis first discussed in Ref. [6].

Note added. After the completion of this work, other authors have independently presented a security analysis of CV MDI QKD obtained by exploiting entropic uncertainty relations [38]. Although directly applicable to obtain security against coherent attacks, this approach is known to provide bounds on the secret-key rate that in general are not tight.

ACKNOWLEDGMENTS

This work was supported by the Innovation Fund Denmark within the Quantum Innovation Center Qubiz and the U.K. Quantum Communications hub (EP/M013472/1). C.L. acknowledges the valuable scientific support received from the Quantum Physics and Information Technology Group (QPIT) of the Technical University of Denmark (DTU) and is especially grateful to Anthony Leverrier for insightful comments and discussions.

APPENDIX A: OPERATIONAL INTERPRETATION OF THE SECURITY PARAMETER

Ideally, in QKD one would like to obtain a shared key that is truly random and secret to the eavesdropper. The final state of a protocol that successfully distributes s perfectly secret bits would be represented by a density operator of the form

$$\rho_0 = 2^{-s} \sum_{x=0}^{2^s-1} |x\rangle_A\langle x| \otimes |x\rangle_B\langle x| \otimes \sigma_E. \tag{A1}$$

In reality, one can only hope to get as close as possible to such an ideal scenario. Let ρ denote the final state of a given QKD protocol. The extent to which the state ρ approximates the ideal one ρ_0 is often quantified in terms of the trace distance:

$$D(\rho,\rho_0) = \tfrac{1}{2}\|\rho - \rho_0\|_1 = \tfrac{1}{2}\mathrm{Tr}|\rho - \rho_0|\,. \tag{A2}$$

The trace distance has several desirable properties for a good security quantifier [29,39,40]. In particular, here we discuss its interpretation in terms of the probability that the generated key is secret. It is well known that the operational meaning of the trace distance is related to the problem of quantum state discrimination [41]. Suppose one is given a black box containing either ρ or ρ_0, each with probability $1/2$. Then any measurement strategy, compatible with the principles of quantum mechanics, allows one to distinguish between the two states up to an error probability [42]

$$p_e \geqslant \frac{1 - D(\rho,\rho_0)}{2}. \tag{A3}$$

Let us define a binary random variable U with probability distribution $P_U = (p_e, 1 - p_e)$. As a matter of fact U characterizes the distinguishability of the states ρ and ρ_0, that is, between the output of the given QKD protocol and an ideal, perfectly secure one. For example, if the state happens to coincide with the ideal one, we have $P_U = P_{\mathrm{sec}} = (1/2, 1/2)$. On the other hand, if the state can be perfectly distinguished from the ideal one, $P_U = P_{\mathrm{insec}} = (0,1)$.

Putting $D(\rho,\rho_0) = \epsilon$ we can write

$$P_U = \left(\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right) = (1-\epsilon)P_{\mathrm{sec}} + \epsilon P_{\mathrm{insec}}. \tag{A4}$$

Therefore, the probability distribution of the variable U characterizing the output of the QKD protocol is the convex sum of the probability distribution P_{sec} associated to the ideal output state and the probability P_{insec} associated to a state that can be perfectly distinguished from the ideal one. In conclusion, such a convex sum decomposition of P_U allows us to interpret $1 - \epsilon$ as the probability that the output of the QKD protocol is indistinguishable from the ideal one, and thus for all practical purposes is itself perfectly secure. In other words, the probability that the output of the protocol is not perfectly secure is smaller than ϵ. Assuming the worst-case scenario, below we put ϵ equal to the probability that the key is not secret.

Taking abstraction on the state and focusing on the protocol itself, this same reasoning is extended to the direct comparison of two protocols $\mathcal{E}$ and $\mathcal{E}_0$, formally represented as completely positive maps, via the diamond norm

$$\|\mathcal{E} - \mathcal{E}_0\|_\diamond = \sup_\sigma \|(\mathcal{E}\otimes I - \mathcal{E}_0 \otimes I)\sigma\|_1, \tag{A5}$$

where the supremum is over all input states and the maps are extended to include an ancillary system.

APPENDIX B: SOME PROPERTIES OF SMOOTH ENTROPY

One of the main tools for quantifying the security of QKD is the conditional smooth min-entropy. In this Appendix we review some of the main definitions and properties (see Refs. [29,30] for the proofs) and derive a useful inequality in Proposition 6 that is applied for our security proof.

Definition 2: Conditional min-entropy. The min-entropy of A conditioned on B of the bipartite state ρ_{AB} is

$$H_{\min}(A|B)_\rho := \max_\sigma \sup\{\lambda : \rho_{AB} \leqslant 2^{-\lambda} I_A \otimes \sigma_B\}, \tag{B1}$$

where I is the identity operator and σ is a subnormalized state.

Here we are interested in the conditional min-entropy of classical-quantum (CQ) states of the form $\rho_{XB} = \sum_{x\in\mathcal{X}} P(x)|x\rangle\langle x| \otimes \omega(x)$. In this case the conditional min-entropy can be written in terms of the maximum guessing probability:

$$2^{-H_{\min}(X|B)_\rho} = \max_{\mathcal{E}} \sum_{x\in\mathcal{X}} P(x)\langle x|\mathcal{E}(\omega(x))|x\rangle, \tag{B2}$$

where $\mathcal{E}$ is a quantum channel.

The following holds:

Lemma 1. Let $\rho = \sum_{x\in\mathcal{X}} P(x)|x\rangle\langle x| \otimes \omega(x)$ be a CQ state and $\mathcal{S}$ a subset of $\mathcal{X}$. We define the projector operator $\Pi = \sum_{x\in\mathcal{S}} |x\rangle\langle x|$, and the state $p^{-1}\Pi\rho\Pi$, with $p = \mathrm{Tr}(\Pi\rho\Pi)$. The following inequality holds:

$$H_{\min}(X|B)_{p^{-1}\Pi\rho\Pi} \geqslant H_{\min}(X|B)_\rho + \log p. \tag{B3}$$

Proof. By applying the characterization of the min-entropy in terms of the guessing probability, we obtain

$$\begin{aligned} 2^{-H_{\min}(X|B)_{p^{-1}\Pi\rho\Pi}} &= \max_{\mathcal{E}} \sum_{x\in\mathcal{S}} p^{-1} P(x)\langle x|\mathcal{E}(\omega(x))|x\rangle && \text{(B4)}\\ &\leqslant p^{-1} \max_{\mathcal{E}} \sum_{x\in\mathcal{X}} P(x)\langle x|\mathcal{E}(\omega(x))|x\rangle && \text{(B5)}\\ &= p^{-1} 2^{-H_{\min}(X|B)_\rho} && \text{(B6)}\\ &= 2^{-H_{\min}(X|B)_\rho - \log p}. && \text{(B7)} \end{aligned}$$

■

The smooth conditional min-entropy of ρ is defined as the maximum min-entropy in a neighborhood of ρ:

Definition 3: Smooth conditional min-entropy. The smooth conditional min-entropy of A conditioned on B of the state ρ_{AB} is

$$H^\epsilon_{\min}(A|B)_\rho := \max_{\tilde\rho} H_{\min}(A|B)_{\tilde\rho}, \tag{B8}$$

where $\tilde\rho$ is a "smoothing state" such that $D(\tilde\rho,\rho) \leqslant \epsilon$, with $D(\tilde\rho,\rho)$ denoting the trace distance.

Remark 4. Here we have defined the entropy smoothing using the trace distance as in Ref. [29] instead of the purified distance as done in Ref. [30].

Remark 5. For a CQ state ρ it is sufficient to consider smoothing states that are classical on the same support as ρ [30]. Therefore, there exists a CQ state $\rho_\star$ such that $D(\rho_\star,\rho) \leqslant \epsilon$ and

$$H^\epsilon_{\min}(X|B)_\rho = H_{\min}(X|B)_{\rho_\star}. \tag{B9}$$

Lemma 2. Let us consider two CQ states $\rho = \sum_{x\in\mathcal{X}} P(x)|x\rangle\langle x| \otimes \omega(x)$ and $\rho_\star = \sum_{x\in\mathcal{X}} P_\star(x)|x\rangle\langle x| \otimes \omega_\star(x)$ such that $D(\rho,\rho_\star) \leqslant \epsilon$, and a projector operator $\Pi = \sum_{x\in\mathcal{S}} |x\rangle\langle x|$. Then $D(p^{-1}\Pi\rho\Pi, p_\star^{-1}\Pi\rho_\star\Pi) \leqslant \frac{3}{2}p^{-1}\epsilon$, where $p = \mathrm{Tr}(\Pi\rho\Pi) = \sum_{x\in\mathcal{S}} P(x)$ and $p_\star = \mathrm{Tr}(\Pi\rho_\star\Pi) = \sum_{x\in\mathcal{S}} P_\star(x)$.

Proof. First notice that the trace distance between the two CQ states reads

$$D(\rho,\rho_\star) = \sum_{x\in\mathcal{X}} D(P(x)\omega(x), P_\star(x)\omega_\star(x)), \tag{B10}$$

and that $D(\rho,\rho_\star) \leqslant \epsilon$ implies

$$|p - p_\star| \leqslant \epsilon. \tag{B11}$$

We then have

$$\begin{aligned} &D\left(p^{-1}\Pi\rho\Pi, p_\star^{-1}\Pi\rho_\star\Pi\right)\\ &= \sum_{x\in\mathcal{S}} D(p^{-1}P(x)\omega(x), p_\star^{-1}P_\star(x)\omega_\star(x)) && \text{(B12)}\\ &\leqslant \sum_{x\in\mathcal{S}} D(p^{-1}P(x)\omega(x), p^{-1}P_\star(x)\omega_\star(x))\\ &\quad + D(p^{-1}P_\star(x)\omega_\star(x), p_\star^{-1}P_\star(x)\omega_\star(x)) && \text{(B13)}\\ &= \sum_{x\in\mathcal{S}} p^{-1} D\left(P(x)\omega(x), P_\star(x)\omega_\star(x)\right)\\ &\quad + \frac{1}{2}|p^{-1} - p_\star^{-1}|P_\star(x)\|\omega_\star(x)\|_1 && \text{(B14)}\\ &= \sum_{x\in\mathcal{S}} p^{-1} D\left(P(x)\omega(x), P_\star(x)\omega_\star(x)\right)\\ &\quad + \frac{1}{2}p^{-1}p_\star^{-1}\,|p - p_\star|\,P_\star(x) && \text{(B15)}\\ &\leqslant p^{-1}\epsilon + \frac{1}{2}p^{-1}\epsilon && \text{(B16)}\\ &= \frac{3}{2}p^{-1}\epsilon, && \text{(B17)} \end{aligned}$$

where in the first inequality we have applied the triangular inequality and in the last one we have applied Eqs. (B10) and (B11). ■

We are now ready to present a "smoothed" version of Lemma 1:

Proposition 6. Let $\rho = \sum_{x\in\mathcal{X}} P(x)|x\rangle\langle x| \otimes \omega(x)$ be a CQ state and $\mathcal{S}$ a subset of $\mathcal{X}$. We define the projector $\Pi = \sum_{x\in\mathcal{S}} |x\rangle\langle x|$, and the (normalized) state $\tau = p^{-1}\Pi\rho\Pi$, where $p = \mathrm{Tr}(\Pi\rho\Pi)$. The following inequality relates the conditional smooth min-entropies of ρ and τ:

$$H^\epsilon_{\min}(X|B)_{p^{-1}\Pi\rho\Pi} \geqslant H^{\frac{2}{3}p\epsilon}_{\min}(X|B)_\rho + \log\left(p - \frac{2}{3}p\epsilon\right). \tag{B18}$$

Proof. Let $\rho_\star$ be a CQ state such that $D(\rho,\rho_\star) \leqslant \frac{2}{3}p\epsilon$. Lemma 2 implies that $D(p^{-1}\Pi\rho\Pi, p_\star^{-1}\Pi\rho_\star\Pi) \leqslant \epsilon$. We then upper-bound the conditional smooth min-entropy of $\tau = p^{-1}\Pi\rho\Pi$ as follows:

$$\begin{aligned} H^\epsilon_{\min}(X|B)_{p^{-1}\Pi\rho\Pi} &\geqslant H_{\min}(X|B)_{p_\star^{-1}\Pi\rho_\star\Pi} && \text{(B19)}\\ &\geqslant H_{\min}(X|B)_{\rho_\star} + \log p_\star && \text{(B20)}\\ &= H^{\epsilon'}_{\min}(X|B)_\rho + \log p_\star && \text{(B21)}\\ &\geqslant H^{\epsilon'}_{\min}(X|B)_\rho + \log(p - \epsilon'), && \text{(B22)} \end{aligned}$$

where in the first inequality we have applied the fact that $p_\star^{-1}\Pi\rho_\star\Pi$ is ϵ-close to $p^{-1}\Pi\rho\Pi$, in the second inequality we have applied Lemma 1, the first equality is obtained choosing a $\rho_\star$ that verifies Eq. (B9) with $\epsilon' = \frac{2}{3}p\epsilon$, and the last inequality is obtained from Eq. (B11). ■

1. Dealing with the nonzero probability that the protocol aborts

The assumption that the state $\rho^{\otimes n}$ is a tensor product is justified for collective attacks. However, since error correction has a nonzero probability of aborting, one should consider the conditional probability of obtaining a secret key given the protocol did not abort. Unfortunately, the state conditioned on the protocol not aborting is no longer guaranteed to have a tensor product structure.

The state $\rho^{\otimes n}$, which describes the correlations between Bob's output measurement and Eve, is a CQ state of the form

$$\rho^{\otimes n} = \sum_{x^n y^n} P(x^n, y^n)|x^n\rangle\langle x^n| \otimes |y^n\rangle\langle y^n| \otimes \omega_E(x^n y^n), \tag{B23}$$

where $P(x^n, y^n)$ is the probability of a sequence of symbols x^n, y^n and $\omega_E(x^n y^n)$ is the corresponding conditional state of Eve. The protocol does not abort only on a given subset $\mathcal{S}$ of the sequences $x^n y^n$; therefore, the state for a nonaborting protocol reads

$$\tau^n = p^{-1}\Pi\rho^{\otimes n}\Pi, \tag{B24}$$

where $\Pi = \sum_{x^n y^n \in \mathcal{S}} |x^n\rangle\langle x^n| \otimes |y^n\rangle\langle y^n|$ is a projector operator, and $p = \mathrm{Tr}(\Pi\rho^{\otimes n}\Pi)$ is the normalization factor.

Proposition 6 yields a simple relation between the conditional smooth min-entropies of $\rho^{\otimes n}$ and τ^n, namely,

$$H_{\min}^{\epsilon}(X|E)_{\tau^n} \geqslant H_{\min}^{\frac{2}{3}p\epsilon}(X|E)_{\rho^{\otimes n}} + \log\left(p - \frac{2}{3}p\epsilon\right), \tag{B25}$$

where p is interpreted as the probability that the protocol does not abort.

APPENDIX C: TAIL BOUNDS

The cumulative distribution function of the χ-squared variable $\chi^2(k)$ with k degrees of freedom is $F(x;k) = \frac{\Gamma[k/2,x/2]}{\Gamma[k/2]}$, where $\Gamma[k/2]$ is the Euler gamma function, and $\Gamma[k/2,x/2]$ is the lower incomplete gamma function.

To bound the cumulative distribution function we can use, for example, the tail bounds:

$$\Pr\left\{k < \frac{\chi}{1+t}\right\} < e^{-nt^2/8}, \tag{C1}$$

$$\Pr\left\{k > \frac{\chi}{1-t}\right\} < e^{-nt^2/8}. \tag{C2}$$

(These bounds are derived from the Chernoff bound using the fact that the distribution of $\chi^2(k)$ is subexponential with parameters $(2\sqrt{k},4)$).

A direct application of these bounds yields

$$\Pr\left\{\langle q_Z^2\rangle < \frac{n^{-1}\sum_j q_{Zj}^2}{1+t}\right\} \leqslant e^{-nt^2/8}, \tag{C3}$$

$$\Pr\left\{\langle q_Z^2\rangle > \frac{n^{-1}\sum_j q_{Zj}^2}{1-t}\right\} \leqslant e^{-nt^2/8}, \tag{C4}$$

together with similar bounds for the quantities $\langle p_Z^2\rangle$, $\langle q_A^2\rangle$, $\langle p_A^2\rangle$, $\langle q_B^2\rangle$, and $\langle p_B^2\rangle$.

We also obtain

$$\begin{aligned}\Pr&\left\{\langle q_Z p_Z\rangle > \frac{n^{-1}\sum_j (q_{Zj}+p_{Zj})^2}{4(1-t)} - \frac{n^{-1}\sum_j (q_{Zj}-p_{Zj})^2}{4(1+t)}\right\}\\ &\leqslant \Pr\left\{\langle (q_Z+p_Z)^2\rangle > \frac{n^{-1}\sum_j (q_{Zj}+p_{Zj})^2}{(1-t)}\right\} + \Pr\left\{\langle (q_Z-p_Z)^2\rangle < \frac{n^{-1}\sum_j (q_{Zj}-p_{Zj})^2}{(1+t)}\right\} \leqslant 2e^{-nt^2/8},\end{aligned} \tag{C5}$$

and analogously

$$\Pr\left\{\langle q_Z p_Z\rangle < \frac{n^{-1}\sum_j (q_{Zj}+p_{Zj})^2}{4(1+t)} - \frac{n^{-1}\sum_j (q_{Zj}-p_{Zj})^2}{4(1-t)}\right\} \leqslant 2e^{-nt^2/8}. \tag{C6}$$

This implies

$$\Pr\{x > x_{\max}\} \leqslant 2e^{-nt^2/8}, \quad \Pr\{y > y_{\max}\} \leqslant 2e^{-nt^2/8}, \quad \Pr\{z < z_{\min}\} \leqslant 4e^{-nt^2/8}, \tag{C7}$$

with

$$x_{\max} = \frac{1}{1-t}\sum_j \frac{q_{Aj}^2 + p_{Aj}^2}{2n}, \quad y_{\max} = \frac{1}{1-t}\sum_j \frac{q_{Bj}^2 + p_{Bj}^2}{2n}, \tag{C8}$$

and

$$z_{\min} = \min_{s_1,s_2,s_3\in\{-1,1\}} \left| w_1 \frac{n^{-1}\sum_j q_{Zj}^2}{1+s_1 t} + w_2 \frac{n^{-1}\sum_j p_{Zj}^2}{1+s_2 t} + w_3\left(\frac{n^{-1}\sum_j (q_{Zj}+p_{Zj})^2}{4(1+s_3 t)} - \frac{n^{-1}\sum_j (q_{Zj}-p_{Zj})^2}{4(1-s_3 t)}\right)\right|, \tag{C9}$$

where w_1, w_2, and w_3 are defined in Eqs. (17)–(19).

For example, putting

$$t = \sqrt{\frac{8 \ln (8/\epsilon_{\mathrm{PE}})}{n}}, \tag{C10}$$

we finally obtain

$$\Pr\{x > x_{\max} \vee y > y_{\max} \vee z < z_{\min}\} \leqslant \epsilon_{\mathrm{PE}}. \tag{C11}$$

[1] H. J. Kimble, Nature (London) **453**, 1023 (2008).

[2] S. Pirandola and S. L. Braunstein, Nature (London) **532**, 169 (2016).

[3] S. Pirandola *et al.*, Nat. Photonics **9**, 641 (2015).

[4] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, Nat. Phys. **11**, 713 (2015).

[5] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012); H.-K. Lo, M. Curty, and B. Qi, *ibid.* **108**, 130503 (2012).

[6] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).

[7] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 773 (2015).

[8] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017); see also arXiv:1510.08863.

[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[10] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[11] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012); **112**, 019902(E) (2014).

[13] F. Furrer, Phys. Rev. A **90**, 042325 (2014).

[14] M. Berta, F. Furrer, and V. B. Scholz, J. Math. Phys. **57**, 015213 (2016).

[15] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Phys. Rev. A **93**, 022325 (2016).

[16] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, arXiv:1709.06988.

[17] We put $\hbar = 1$ and assume the commutation relations of the form $[q,p] = 2i$ [18]. In this way the output of homodyne detection over the vacuum state is a Gaussian variable with variance 1.

[18] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).

[19] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, arXiv:1712.00743 [Phys. Rev. Lett. (to be published)].

[20] For simplicity, here we have assumed that $\langle q_Z \rangle = \langle p_Z \rangle = 0$. Otherwise, one must replace $\langle q_Z^2 \rangle \to \langle q_Z^2 \rangle - \langle q_Z \rangle^2$ and $\langle p_Z^2 \rangle \to \langle p_Z^2 \rangle - \langle p_Z \rangle^2$.

[21] It is obvious that they still require to communicate the entries of the CM that have been locally estimated. The CM, however, only contains a negligible amount of information about the local raw keys.

[22] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, and N. Kulesza, New J. Phys. **16**, 013047 (2014).

[23] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[24] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).

[25] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).

[26] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).

[27] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Phys. Rev. A **96**, 042334 (2017).

[28] As a matter of fact, the application of the ADC introduces a quantization error and does not preserve Gaussianity. The effects on the quantization error in parameter estimation will be discussed in detail in a future work.

[29] R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005, arXiv:quant-ph/0512258.

[30] M. Tomamichel, Ph.D. thesis, Swiss Federal Institute of Technology (ETH), Zurich, 2012, arXiv:1203.2142.

[31] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).

[32] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[33] Notice that Theorem 1 of Ref. [10] contains a typographical error, where $4(d+1)\log_2 2/\epsilon^2$ appears instead of $4(d+1)\sqrt{\log_2 2/\epsilon^2}$ in the expression for $\Delta_{\mathrm{AEP}}^{(1)}$. This typo is introduced in Eq. (56) of the Supplemental Material of Ref. [10].

[34] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[35] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[36] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, arXiv:1702.07740.

[37] X. Wang, Y.-C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, Quantum Inf. Comput. **17**, 1123 (2017).

[38] Y. Zhao, Y.-C. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).

[39] R. Renner and R. König, *Second Theory of Cryptography Conference TCC*, Lecture Notes in Computer Science Vol. 3378 (Springer, New York, 2005), pp. 407–425.

[40] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).

[41] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976)

[42] More recently, the purified distance $P(\rho,\rho_0)$ was employed instead of the trace distance [30]. However, since $D(\rho,\rho_0) \leqslant P(\rho,\rho_0)$ we still have $p_e \geqslant \frac{1}{2}(1 - D(\rho,\rho_0)) \geqslant \frac{1}{2}(1 - P(\rho,\rho_0))$.